UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MICHIGAN

NATHAN SILVA, *individually and on behalf of all others similarly situated*, Plaintiff, v. FLAGSTAR BANK, FSB, Defendant.	Case No. _____ **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiff Nathan Silva ("Plaintiff"), individually and on behalf of all others similarly situated, brings this Class Action Complaint against Defendant Flagstar Bank, FSB ("Flagstar" or "Defendant"). Plaintiff alleges the following upon information and belief based on the investigation of counsel, except as to those allegations that specifically pertain to Plaintiff, which are alleged upon personal knowledge.

NATURE OF THE ACTION

1. This is a class action brought by Plaintiff on behalf of similarly situated individuals (the "Class," as defined below) who entrusted Flagstar with sensitive personal information which was subsequently exposed in a data breach that was discovered by Flagstar on June 2, 2022. *See Flagstar Standard Notification Letter*, https://bit.ly/3ATGtKB (last visited July 15, 2022).

2. Between December 3, 2021, and December 4, 2021, hackers accessed Flagstar's networks and servers and exfiltrated highly-sensitive personal information of more than 1.5 million U.S. customers (the "Data Breach").

3. The Data Breach was a result of Flagstar's failure to properly secure and safeguard Plaintiff's and the Class members' sensitive personal information stored within its network and servers, including, without limitation, full names, Social Security numbers, and phone numbers (collectively, "personally identifiable information" or "PII").

4. On June 2, 2022, approximately six months after the Data Breach took place, Flagstar discovered that an unauthorized third party had gained access to Flagstar's network. *Flagstar Standard Notification Letter*, https://bit.ly/3ATGtKB (last visited July 15, 2022).

5. Flagstar began notifying affected individuals that their PII was compromised over two weeks later on, June 17, 2022. *See, e.g.*, OFFICE OF THE MAINE ATTORNEY GENERAL, *Data Breach Notifications* (2022), https://bit.ly/3uR6l66 (last visited July 15, 2022).

6. At this time, it is unclear if Flagstar has provided notice to all impacted individuals.

7. Plaintiff received a Notice of Data Breach letter from Flagstar dated June 15, 2022. Attached hereto as Exhibit 1 is a copy of Plaintiff's notice letter.

8. As of the time Flagstar filed its Data Breach Notification with the State of Maine in June, 1,547,169 United States residents were affected by the Data Breach. OFFICE OF THE MAINE ATTORNEY GENERAL, *Data Breach Notifications* (2022), https://bit.ly/3uR6l66 (last visited July 15, 2022).

9. Defendant maintained the PII in a reckless and negligent manner. In particular, the PII was maintained on Defendant's network system in a condition vulnerable to cyberattacks.

10. Defendant exposed Plaintiff and the Class members to harm by intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust network systems and security practices in place to safeguard participants' PII; failing to take standard and reasonably available steps to prevent the Data Breach from occurring; failing to quickly detect the Data Breach; and failing to promptly notify Plaintiff and the Class members of the Data Breach.

11. Plaintiff and the Class members are now subject to the present and continuing risk of identity theft and fraud.

12. According to Experian, one of the largest credit reporting companies in the world, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to, among other things, open

a new credit card or loan; change a billing address so the victim no longer receives bills; open new utilities in the victim's name; obtain a mobile phone; open a bank account and write bad checks; use a debit card number to withdraw funds; obtain a new driver's license or ID; or use the victim's information in the event of arrest or court action. Susan Henson, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself?*, WWW.EXPERIAN.COM (Sept. 1, 2017), https://bit.ly/3Obrlvg.

13. Consumers who trusted Flagstar to securely store their information have suffered injury and ascertainable losses in the form of the present and imminent threat of fraud and identity theft, increased risk of future identity theft and fraud, out-of-pocket expenses and value of time reasonably incurred to remedy or mitigate the effects of the Data Breach, loss of value of their personal information, and loss of the benefit of their bargain.

14. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Class members' PII that Defendant collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and the other Class members that their information had been subject to the unauthorized access of an unknown third party.

15. Plaintiff and the Class members have a continuing interest in ensuring their information is, and remains, safe. On behalf of the Class, Plaintiff seeks

monetary and injunctive and other equitable relief, and he demands a trial by jury.

PARTIES

16. Plaintiff Nathan Silva is a resident of Muskegon, Michigan.

17. Plaintiff received a Notice of Data Breach letter from Flagstar dated June 15, 2022. Attached hereto as Exhibit 1 is a copy of Plaintiff's notice letter.

18. Prior to receiving the Notice of Data Breach letter in June 2022, Plaintiff shared his PII with Flagstar in order to open up a business account for the business which he owns and operates, Nth Power Designs, LLC.

19. Plaintiff's Notice of Data Breach letter of June 15, 2022, indicates Flagstar determined Plaintiff's PII, including, at a minimum, "Social Security number, name, and phone number," was part of the Data Breach. Ex. 1 [Plaintiff's Notice of Data Breach letter].

20. Plaintiff suffered injury and was damaged as a result of Flagstar's failure to keep his PII secure.

21. Defendant Flagstar Bank, FSB, is a federally chartered savings bank organized under the laws of the state of Michigan with its principal place of business located at 5151 Corporate Drive, Troy, Michigan 48098.

JURISDICTION AND VENUE

22. This Court has original subject matter jurisdiction over this proposed class action pursuant to the Class Action Fairness Act of 2005, under 28 U.S.C. §

1332(d). At least one member of the nationwide plaintiff class is a citizen of a State different from Defendant, and the matter in controversy is exceeds $5,000,000 in the aggregate, exclusive of interest and costs. Further, the number of members of all proposed plaintiff classes in the aggregate is greater than 100.

23. This Court has personal jurisdiction over Defendant because Defendant is headquartered in Michigan and conducts substantial business in Michigan through its headquarters, offices, parents, and affiliates.

24. Venue is also proper in this District pursuant to 28 U.S.C. § 1391, because Defendant is headquartered in this District, and a substantial part of the events giving rise to Plaintiff's claims occurred in this District.

ALLEGATIONS COMMON TO ALL CLAIMS

I. Flagstar Advertises Its Record Retention Services as Secure

25. Flagstar was chartered in 1987 as a federal savings bank, growing to control assets of $23.2 billion, and becoming the sixth largest bank mortgage originator nationally. FLAGSTAR BANK, *About Flagstar*, WWW.FLAGSTAR.COM (2022), https://www.flagstar.com/about-flagstar.html. Flagstar currently has 150 branches located in Michigan, Indiana, California, Wisconsin, and Ohio, offering a full complement of banking products and services for consumers and businesses. *Id.*

26. Upon information and belief, Flagstar obtains consumers' PII to provide its services. As a part of this exchange, Flagstar's Privacy Policy promises

"[t]o protect your personal information from unauthorized access and use, . . . [using] security measures that comply with federal law. These measures include computer safeguards and secured files and buildings." FLAGSTAR BANK, *About Your Privacy* (Feb. 2018), https://bit.ly/3PprgoY.

27. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and the Class members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and the Class members' PII from unauthorized access and disclosure.

28. Plaintiff and the Class members have taken reasonable steps to maintain the confidentiality of their PII.

29. Plaintiff and the Class members relied on Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

II. Flagstar's Electronic Record Security Has Been Breached in the Recent Past

30. The Data Breach at issue in the case at bar is the second major incident to affect Flagstar and its customers in less than a year. In January 2021, a notorious hacking group named "Clop" breached the servers of Flagstar's vendor, Accellion, and accessed the customer data of 1.48 million Flagstar employees and customers.

31. This breach resulted in Flagstar being extorted by Clop through a ransomware attack, its customers having their data exposed to cybercriminals, and

ended the collaboration between Flagstar and the Accellion platform.

32. After Flagstar began notifying victims of the data breach starting in March of 2021, the hacking group released screenshots of stolen personal data including Social Security numbers, names, addresses, phone numbers, and tax records—with a warning that it had stolen a lot more.

33. Flagstar was named as a defendant in five separate putative class actions relating to the breach and ultimately settled those cases in late 2021.

III. Flagstar's Electronic Record Security Was Breached with Respect to Plaintiff's and the Class Members' PII

34. On June 2, 2022, Flagstar "discovered . . . that certain impacted files containing [Plaintiff's and the Class members'] personal information were accessed and/or acquired from [its] network between December 3, 2021 and December 4, 2021." Ex. 1 [cite to Plaintiff's Notice of Data Breach letter].

35. On June 2, 2022, Flagstar determined Plaintiff's and the Class members' PII, including, at a minimum, "Name or other personal identifier in combination with: **Social Security Number**," was exposed in the Data Breach. OFFICE OF THE MAINE ATTORNEY GENERAL, *Data Breach Notifications* (2022), https://bit.ly/3uR6l66 (last visited July 15, 2022).

36. By June 17, 2022, Flagstar notified the Maine Attorney General's Office and began sending out notifications to impacted individuals. *Id.*

37. At this time, it is unclear whether Flagstar has notified all affected

consumers.

IV. Flagstar's Response Increased the Potential for Harm

38. As a result of Flagstar's inability to secure Plaintiff's and the Class members' PII, Plaintiff and the Class members are now subject to the present and continuing risk of identity theft and fraud. Defendant could have prevented this Data Breach by properly securing and encrypting the PII of Plaintiff and the Class members.

39. Enhancing the danger to Plaintiff and the Class, Flagstar was incapable of detecting the Data Breach for six months.

40. While Flagstar discovered the Data Breach on June 2, 2022, at Plaintiff's and the Class members' expense, it took an additional 15 days for Flagstar to start notifying impacted consumers. OFFICE OF THE MAINE ATTORNEY GENERAL, *Data Breach Notifications* (2022), https://bit.ly/3uR6l66 (last visited July 15, 2022).

41. Flagstar's own efforts to ameliorate the damage it caused by failing to secure Plaintiff's and the Class members' PII culminated in the inadequate offer of credit monitoring services for two years. *See Flagstar Standard Notification Letter*, https://bit.ly/3ATGtKB (last visited July 15, 2022).

V. Plaintiff and the Class Members Were Damaged as a Result of Flagstar's Actions and Inactions

42. Plaintiff and the Class members have been damaged by the compromise of their PII in the Data Breach, including, at minimum, names or personal identifiers

in combination with Social Security numbers.

43. Social Security numbers are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, when they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought.
>
> Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.

SOCIAL SECURITY ADMINISTRATION, *Identity Theft and Your Social Security Number* (July 2021), https://www.ssa.gov/pubs/EN-05-10064.pdf.

44. The PII of Plaintiff and the Class members was taken by hackers in the Data Breach to engage in identity theft and/or to sell it to other criminals who will purchase the PII for that purpose.

45. The PII of individuals is of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.

Anita George, *Your personal data is for sale on the dark web. Here's how much it costs*, WWW.DIGITALTRENDS.COM (Oct. 16, 2019), https://bit.ly/3aOrhE6. Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web. Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, WWW.EXPERIAN.COM (Dec. 6, 2017), https://bit.ly/3zbkk9A. Criminals can also purchase access to ongoing entire company data breaches from $900 to $4,500. *In the Dark*, VPNOVERVIEW.COM (2019), https://bit.ly/3caOgJI.

46. Because it includes personal identifiers and Social Security numbers, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, because victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—name, Social Security number, and potentially date of birth.

47. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market." Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, WWW.NETWORKWORLD.COM (Feb. 6, 2015), https://bit.ly/3AS0Ms2.

48. The fraudulent activity resulting from the Data Breach may not come

to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

U.S. GOVERNMENT ACCOUNTABILITY OFFICE, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), https://www.gao.gov/assets/gao-07-737.pdf.

49. Plaintiff and the Class members presently face substantial risk of imminent out-of-pocket fraud losses such as loans opened in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

50. Plaintiff and the Class members have been, and currently face substantial risk of being, targeted now and in the future, subjected to phishing, data intrusion, and other illegality based on their PII, as potential fraudsters could use that information to target such schemes more effectively to Plaintiff and the Class members.

51. Plaintiff and the Class members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze

fees, and similar costs directly or indirectly related to the Data Breach.

52. Plaintiff and the Class members also suffered a loss of value of their PII when it was acquired by cyber thieves in the Data Breach.

53. Plaintiff and the Class members have spent and will continue to spend significant amounts of time to monitor their financial accounts and records for misuse.

54. Plaintiff and the Class members have suffered or will imminently suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

55. Moreover, Plaintiff and the Class members have an interest in ensuring that their PII, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to making sure that the storage of data or documents containing personal and financial information is not accessible online and that access to such data is password protected.

56. Furthermore, as a result of Defendant's conduct, Plaintiff and the Class members are forced to live with the anxiety that their PII—which contains the most intimate details about a person's life—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy

whatsoever.

57. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and the Class members have suffered anxiety, emotional distress, and are at an increased risk of future harm.

CLASS ACTION ALLEGATIONS

58. Pursuant to Rule 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure, Plaintiff brings this action on behalf of a proposed class defined as follows:

> **The Nationwide Class.** All natural persons residing in the United States who are current or former customers of Flagstar whose PII was compromised as a result of the December 2021 Data Breach.
>
> Excluded from the Nationwide Class are: (a) Defendant, Defendant's board members, executive-level officers, attorneys, and immediate family members of any of the foregoing persons; (b) governmental entities; (c) the Court, the Court's immediate family, and the Court staff; and (d) any person that timely and properly excludes himself or herself from the Class in accordance with Court-approved procedures.

59. Additionally, or in the alternative, pursuant to Rule 23(a), (b)(2), and (b)(3), Plaintiff brings this action on behalf of a proposed subclass defined as follows:

> **The Michigan Subclass.** All natural persons residing in Michigan who are current or former customers of Flagstar whose PII was compromised as a result of the December 2021 Data Breach.
>
> Excluded from the Michigan Subclass are: (a) Defendant, Defendant's board members, executive-level officers, attorneys, and immediate family members of any of the foregoing persons; (b) governmental

entities; (c) the Court, the Court's immediate family, and the Court staff; and (d) any person that timely and properly excludes himself or herself from the Class in accordance with Court-approved procedures.

60. Together, the Nationwide Class and the Michigan Subclass are the "Class."

61. Plaintiff reserves the right to amend the Class definition above if further investigation and/or discovery reveals that the Class should be expanded, narrowed, divided into subclasses, or otherwise modified in any way.

62. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of his claims on a class-wide basis using the same evidence as individual Class members would use to prove those elements in individual actions alleging the same claims.

i. **Numerosity—Federal Rule of Civil Procedure 23(a)(1).** The proposed Class is sufficiently numerous that individual joinder of all Class members is impracticable. Plaintiffs believe that there are approximately one million, five hundred thousand (1,500,000) Class members. The precise number of Class members is presently unknown to Plaintiffs, but may be ascertained from Defendant's books, records, and electronically stored information. Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. Mail, electronic mail, Internet postings, and/or published notice. **Commonality and Predominance—Federal Rules of Civil Procedure 23(a)(2) and 23(b)(3).** This action involves common questions of law and fact, which predominate over any questions affecting only individual Class members, including, without limitation: whether Defendant engaged in the conduct alleged herein;

ii. whether Defendant failed to implement and maintain reasonable

security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

iii. whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

iv. whether Defendant breached implied contracts it had with Plaintiff and the Class members;

v. whether Defendant's conduct was negligent;

vi. whether Defendant's conduct violated Plaintiff's and the Class members' privacy;

vii. whether Flagstar took sufficient steps to secure its customers' PII;

viii. whether Plaintiff and the Class members are entitled to actual or other forms of damages and other monetary relief; and

ix. whether Plaintiff and the Class members are entitled to equitable relief, including but not limited to injunctive relief.

63. **Typicality—Federal Rule of Civil Procedure 23(a)(3).** Plaintiff's claims are typical of the claims of the Class members because Defendant injured all Class members through the uniform misconduct described herein; all Class members were subject to Flagstar's inadequate handling of their PII in connection with the December 2021 Data Breach; and Plaintiff seeks the same relief as the Class members.

64. Furthermore, there are no defenses available to Defendant that are unique to Plaintiff.

65. **Adequacy of Representation—Federal Rule of Civil Procedure 23(a)(4).** Plaintiff is a fair and adequate representative of the Class because Plaintiff's interests do not conflict with the Class members' interests. Plaintiff will prosecute this action vigorously and is highly motivated to seek redress against Defendant. Furthermore, Plaintiff has selected competent counsel that are experienced in class action and other complex litigation. Plaintiff and his counsel are committed to prosecuting this action vigorously on behalf of the Class and have the resources to do so.

66. **Declaratory and Injunctive Relief—Federal Rule of Civil Procedure 23(b)(2).** The requirements for maintaining a class action pursuant to Rule 23(b)(2) are met, as Defendant has acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive relief or corresponding declaratory relief with respect to the Class as a whole.

67. Given that Flagstar has not indicated any changes to its conduct or security measures, monetary damages are insufficient and there is no complete and adequate remedy at law.

68. **Superiority—Federal Rule of Civil Procedure 23(b)(3).** The class action mechanism is superior to other available means for the fair and efficient adjudication of this controversy for reasons including but not limited to the following:

i. The damages individual Class members suffered are small compared to the burden and expense of individual prosecution of the complex and extensive litigation needed to address Defendant's conduct.

ii. Further, it would be virtually impossible for the Class members individually to redress effectively the wrongs done to them. Even if Class members themselves could afford such individual litigation, the court system could not. Individualized litigation would unnecessarily increase the delay and expense to all parties and to the court system and presents a potential for inconsistent or contradictory rulings and judgments. By contrast, the class action device presents far fewer management difficulties, allows the hearing of claims which might otherwise go unaddressed because of the relative expense of bringing individual lawsuits, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

iii. The prosecution of separate actions by the individual members of the Class would create a risk of inconsistent or varying adjudications with respect to individual Class members, which would establish incompatible standards of conduct for Defendant.

iv. The prosecution of separate actions by individual Class members would create a risk of adjudications with respect to them that would, as a practical matter, be dispositive of the interests of other Class members not parties to the adjudications or that would substantively impair or impede their ability to protect their interests.

CLAIMS FOR RELIEF

COUNT I
Breach of Implied Contract
By Plaintiff on Behalf of the Class

69. Plaintiff repeats each and every allegation contained in the paragraphs above and incorporates such allegations by reference herein.

70. Plaintiff brings this claim on behalf of the Class for breach of implied contract.

71. In connection with receiving services from Flagstar, Plaintiff and all other Class members entered into implied contracts with Flagstar.

72. Pursuant to these implied contracts, Plaintiff and the Class members provided Flagstar with their PII in order for Flagstar to provide its services, for which Flagstar is compensated. In exchange, Flagstar agreed to, among other things, and Plaintiff and the Class members understood that Flagstar would: (1) provide services to Plaintiff and the Class members; (2) take reasonable measures to protect the security and confidentiality of Plaintiff's and the Class members' PII; and (3) protect Plaintiff's and the Class members' PII in compliance with federal and state laws and regulations and industry standards.

73. In the ordinary course of providing its services, customers provide Defendant with PII, including names and Social Security numbers.

74. Implied in these exchanges was a promise by Defendant to ensure that the PII of Plaintiff and the Class members in its possession was secure.

75. Implied in these exchanges was a promise by Defendant to ensure the PII of Plaintiff and the Class members in its possession was only used to provide the agreed-upon services, and that Defendant would take adequate measures to protect Plaintiff's and the Class members' PII.

76. A material term of this contract is a covenant by Defendant that it would take reasonable efforts to safeguard that information. Defendant breached this covenant by allowing Plaintiff's and the Class members' PII to be accessed in the Data Breach.

77. Indeed, implicit in the agreement between Defendant and its customers was the obligation that both parties would maintain information confidentially and securely.

78. These exchanges constituted an agreement and meeting of the minds between the parties: Plaintiff and the Class members would provide their PII in exchange for services by Defendant. These agreements were made by Plaintiff and the Class members as customers of Defendant.

79. It is clear by these exchanges that the parties intended to enter into an agreement and mutual assent occurred. Plaintiff and the Class members would not have disclosed their PII to Defendant but for the prospect of utilizing Defendant's services. Conversely, Defendant presumably would not have taken Plaintiff's and the Class members' PII if it did not intend to provide Plaintiff and the Class members with its services.

80. Defendant was therefore required to reasonably safeguard and protect the PII of Plaintiff and the Class members from unauthorized access, disclosure, and/or use.

81. Plaintiff and the Class members accepted Defendant's offer of services and fully performed their obligations under the implied contract with Defendant by providing their PII, directly or indirectly, to Defendant, among other obligations.

82. Plaintiff and the Class members would not have entrusted their PII to Defendant in the absence of their implied contracts with Defendant and would have instead retained the opportunity to control their PII.

83. Defendant breached the implied contracts with Plaintiff and the Class members by failing to reasonably safeguard and protect Plaintiff's and the Class members' PII.

84. Defendant's failure to implement adequate measures to protect the PII of Plaintiff and the Class members violated the purpose of the agreement between the parties.

85. Instead of spending adequate financial resources to safeguard Plaintiff's and the Class members' PII, which Plaintiff and the Class members were required to provide to Defendant, Defendant instead used that money for other purposes, thereby breaching its implied contracts it had with Plaintiff and the Class members.

86. As a proximate and direct result of Defendant's breaches of its implied contracts with Plaintiff and the Class members, Plaintiff and the Class members suffered damages as described above.

87. Therefore, Plaintiff prays for relief as set forth below.

COUNT II
Negligence
By Plaintiff on Behalf of the Class

88. Plaintiff repeats each and every allegation contained in the paragraphs above and incorporates such allegations by reference herein.

89. Plaintiff brings this claim on behalf of the Class for negligence.

90. Defendant knowingly collected, came into possession of, and maintained Plaintiff's and the Class members' PII, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

91. Defendant had a duty to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiff's and the Class members' PII.

92. Defendant had, and continues to have, a duty to timely disclose that Plaintiff's and the Class members' PII within its possession was compromised and precisely the type(s) of information that were compromised.

93. Defendant owed a duty of care to Plaintiff and the Class members to provide data security consistent with industry standards, applicable standards of care from statutory authority like Section 5 of the Federal Trade Commission Act, and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the PII.

94. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its customers. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class members from a data breach.

95. Defendant's duty to use reasonable care in protecting confidential data arose because, among other reasons, Defendant is bound by industry standards to protect confidential PII.

96. Defendant breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and the Class members' PII.

97. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

i. failing to adopt, implement, and maintain adequate security measures to safeguard Class members' PII;

ii. failing to adequately monitor the security of its networks and systems; and

iii. failing to periodically ensure that its computer systems and networks had plans in place to maintain reasonable data security safeguards.

98. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and the Class members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and the Class members' PII within Defendant's possession.

99. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and the Class members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiff's and the Class members' PII.

100. Defendant, through its actions and/or omissions, unlawfully breached its duty to timely disclose to Plaintiff and the Class members that the PII within Defendant's possession might have been compromised and precisely the type of information compromised.

101. It was foreseeable that Defendant's failure to use reasonable measures to protect Plaintiff and the Class members' PII would result in injury to Plaintiff and the Class members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches.

102. It was foreseeable that the failure to adequately safeguard Plaintiff's and the Class members' PII would result in injuries to Plaintiff and the Class members.

103. Defendant's breach of duties owed to Plaintiff and the Class members caused Plaintiff's and the Class members' PII to be compromised, in the Data Breach.

104. But for Defendant's negligent conduct and breach of the above-described duties owed to Plaintiff and the Class members, their PII would not have

been compromised.

105. As a result of Defendant's failure to timely notify Plaintiff and the Class members that their PII had been compromised, Plaintiff and the Class members are unable to take the necessary precautions to mitigate damages by preventing future fraud.

106. As a result of Defendant's negligence and breach of duties, Plaintiff and the Class members are in danger of imminent harm in that their PII, which is still in the possession of third parties, will be used for fraudulent purposes, and Plaintiff and the Class members have and will suffer damages including: a substantial increase in the likelihood of identity theft; the compromise, publication, and theft of their personal information; loss of time and costs associated with the prevention, detection, and recovery from unauthorized use of their personal information; the continued risk to their personal information; future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the personal information compromised as a result of the Data Breach; and overpayment for the services that were received without adequate data security.

107. Therefore, Plaintiff prays for relief as set forth below.

COUNT III
Negligence Per Se
By Plaintiff on Behalf of the Class

108. Plaintiff repeats each and every allegation contained in the paragraphs

above and incorporates such allegations by reference herein.

109. Plaintiff brings this claim on behalf of the Class for negligence per se.

110. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect Personal Information. 15 U.S.C. § 45(a)(1).

111. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

112. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Personal Information and not complying with applicable industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of Personal Information it obtained, stored, and disseminated, and the foreseeable consequences of a data breach involving companies as large as Defendant, including, specifically, the immense damages that would result to Plaintiff and the Class members.

113. Defendant's violations of Section 5 of the FTC Act constitute negligence per se.

114. Plaintiff and the Class members are within the class of persons that the FTC Act was intended to protect.

115. The harm that occurred as a result of the Data Breach is the type of

harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class members.

116. As a direct and proximate result of Defendant's negligence per se under the FTC Act, Plaintiff and the Class have suffered, continue to suffer, and will suffer, injuries, damages, and harm as set forth herein.

117. Therefore, Plaintiff prays for relief as set forth below.

COUNT IV
Invasion of Privacy
By Plaintiff on Behalf of the Class

118. Plaintiff repeats each and every allegation contained in the paragraphs above and incorporates such allegations by reference herein.

119. Plaintiff brings this claim on behalf of the Class for invasion of privacy.

120. Plaintiff and the Class members had a legitimate expectation of privacy in their PII and were entitled to the protection of this information against access by and disclosure to unauthorized third parties.

121. Defendant owed a duty to Plaintiff and the Class members to keep their PII contained as a part thereof, confidential.

122. Defendant failed to protect and released to unknown and unauthorized third parties the non-redacted and non-encrypted PII of Plaintiff and the Class

members.

123. Defendant allowed unauthorized and unknown third parties access to and examination of the PII of Plaintiff and the Class members, by way of Defendant's failure to protect the PII.

124. The Personal Information that was publicized during the Data Breach was highly sensitive, private, and confidential, as it included private financial, health, and treatment information. The unauthorized release to, custody of, and examination by unauthorized third parties of the PII of Plaintiff and the Class members is highly offensive to a reasonable person.

125. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and the Class members disclosed their PII to Defendant as part of their relationships with Defendant in order to receive services from Defendant, but privately with an intention that the PII would be kept confidential and would be protected from unauthorized disclosure. Plaintiff and the Class members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

126. The Data Breach at the hands of Defendant constitutes an intentional interference with Plaintiff's and the Class member's interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

127. Defendant acted with a knowing state of mind when it permitted the Data Breach to occur because it was with actual knowledge that its information security practices were inadequate and insufficient.

128. Because Defendant acted with this knowing state of mind, it had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiff and the Class members.

129. As a proximate result of the above acts and omissions of Defendant, the PII of Plaintiff and the Class members was disclosed to third parties without authorization, causing Plaintiff and the Class members to suffer damages.

130. Unless enjoined, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class members in that the PII maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiff and the Class members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and the Class members.

131. Therefore, Plaintiff prays for relief as set forth below.

COUNT V
Breach of Confidence
By Plaintiff on Behalf of the Class

132. Plaintiff repeats each and every allegation contained in the paragraphs above and incorporates such allegations by reference herein.

133. Plaintiff brings this claim on behalf of the Class for breach of confidence.

134. At all times during Plaintiff's and the Class's interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiff's and the Class's PII that Plaintiff and the Class entrusted to Defendant.

135. As alleged herein and above, Defendant's confidential relationship with Plaintiff and the Class was governed by terms and expectations that Plaintiff's and the Class's PII would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties. Such PII was confidential and novel, highly personal and sensitive, and not generally known.

136. Plaintiff and the Class entrusted Defendant with their PII with the explicit and implicit understandings that Defendant would protect and not permit the PII to be disseminated to any unauthorized third parties.

137. Plaintiff and the Class also entrusted Defendant with their PII with the explicit and implicit understandings that Defendant would take precautions to protect that PII from unauthorized access and disclosure.

138. Defendant voluntarily received in confidence Plaintiff's and the Class's PII with the understanding that PII would not be disclosed or disseminated to the public or any unauthorized third parties.

139. Defendant knew Plaintiff's and the Class members' PII was being

disclosed in confidence and understood the confidence was to be maintained, including by expressly and implicitly agreeing to protect the confidentiality and security of the PII it collected, stored, and maintained.

140. Due to Defendant's failure to prevent and avoid the Data Breach from occurring, Plaintiff's and the Class's PII was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and the Class's confidence, and without their express permission.

141. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiff and the Class have suffered damages.

142. But for Defendant's disclosure of Plaintiff's and the Class's PII in violation of the parties' understanding of confidence, their PII would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data Breach was the direct and legal cause of the theft of Plaintiff's and the Class's PII as well as the resulting damages.

143. The injury and harm Plaintiff and the Class suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff's and the Class's PII. Defendant knew or should have known its methods of accepting and securing Plaintiff's and the Class's PII were inadequate as they relate to, at the very least, securing servers and other equipment containing Plaintiff's and the Class's PII.

144. As a direct and proximate result of Defendant's breach of its confidence

with Plaintiff and the Class, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity to control how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual present and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of current and former customers and their beneficiaries and dependents; and (viii) present and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Class members.

145. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of

privacy, and other economic and non-economic losses.

146. Therefore, Plaintiff prays for relief as set forth below.

COUNT VI
Violation of the Michigan Consumer Protection Act
MICH. COMP. LAWS ANN. § 445.901 *et seq.*
By Plaintiff on Behalf of the Michigan Subclass

147. Plaintiff repeats each and every allegation contained in the paragraphs above and incorporates such allegations by reference herein.

148. Plaintiff brings this claim on behalf of the Michigan Subclass for violation of the Michigan Consumer Protection Act, MICH. COMP. LAWS ANN. § 445.901 *et seq.*, which Defendant violated by violating the Michigan Identity Theft Protection Act, MICH. COMP. LAWS ANN. § 445.61 *et seq.*

149. Courts have found that consumers may bring a civil action to enforce the Michigan Identity Theft Protection Act through the Michigan Consumer Protection Act.

150. Under the Michigan Identity Theft Protection Act, "personal information" means the first name or first initial and last name linked to one or more of the following data elements of a resident of Michigan:

i. Social security number;

ii. Driver license number or state personal identification card number;

iii. Demand deposit or other financial account number, or credit card or debit card number, in combination with any required security

> code, access code, or password that would permit access to any of the resident's financial accounts.

MICH. COMP. LAWS ANN. § 445.63(r).

151. Flagstar is a business that owns or licenses computerized data that includes "personal information" as defined under the Michigan Identity Theft Protection Act. *See id.*; MICH. COMP. LAWS ANN. § 445.72(1).

152. Plaintiff's and the Michigan Subclass members' PII includes "personal information" as covered under the Michigan Identity Theft Protection Act. *See* MICH. COMP. LAWS ANN. § 445.63(r).

153. Under the Michigan Identity Theft Protection Act, Flagstar is required to accurately notify Plaintiff and the Michigan Subclass members if it discovers a security breach, or receives notice of a security breach, where unencrypted and unredacted "personal information" was accessed or acquired by unauthorized persons, "without unreasonable delay." MICH. COMP. LAWS ANN. § 445.72(1), (4).

154. Because Flagstar discovered a security breach and had notice of a security breach where unencrypted and unredacted "personal information" was accessed or acquired by unauthorized persons, Flagstar had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by the Michigan Identity Theft Protection Act. MICH. COMP. LAWS ANN. § 445.72(4).

155. By failing to disclose the Data Breach in a timely and accurate manner, Flagstar violated section 445.72(4).

156. As a direct and proximate result of Flagstar's violations of section 445.72(4), Plaintiff and the Michigan Subclass members suffered damages, as described above.

157. Plaintiff and the Michigan Subclass members seek relief under the Michigan Consumer Protection Act for Flagstar's violations of the Michigan Identity Theft Protection Act.

158. Flagstar, Plaintiff, and the Michigan Subclass members are "persons" as defined under the Michigan Consumer Protection Act. *See* MICH. COMP. LAWS ANN. § 445.902(d).

159. Flagstar advertised, offered, or sold goods or services in Michigan and engaged in "trade or commerce" directly or indirectly affecting the people of Michigan, as defined under the Michigan Consumer Protection Act. *See* MICH. COMP. LAWS ANN. § 445.902(g).

160. Flagstar engaged in "[u]nfair, unconscionable, or deceptive methods, acts, or practices in the conduct of trade or commerce," in violation of Michigan Compiled Laws Annotated section 445.903(1).

161. Flagstar's unfair, unconscionable, and deceptive practices include its failure to comply with the Michigan Identity Theft Protection Act.

162. Additionally, Flagstar's deceptive acts, omissions, and conduct include but are not limited to:

i. failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and the Michigan Subclass members' PII, which was a direct and proximate cause of the Data Breach;

ii. failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents in the industry, which were direct and proximate causes of the Data Breach;

iii. failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and the Michigan Subclass members' PII, including but not limited to duties imposed by the Michigan Identity Theft Protection Act, which were direct and proximate causes of the Data Breach;

iv. misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and the Michigan Subclass members' PII, including by implementing and maintaining reasonable security measures;

v. misrepresenting that it would comply with common law, statutory, and self-imposed duties pertaining to the security and privacy of Plaintiff's and the Michigan Subclass members' PII;

vi. omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and the Michigan Subclass members' PII;

vii. omitting, suppressing, and concealing the material fact that it did not comply with common law, statutory, and self-imposed duties pertaining to the security and privacy of Plaintiff's and the Michigan Subclass members' PII; and

viii. failing to promptly and adequately notify Plaintiff and the Michigan Subclass that their PII was accessed by unauthorized persons in the Data Breach.

163. Flagstar had exclusive knowledge of material information regarding its

deficient security policies and practices, and regarding the security of Plaintiff's and the Michigan Subclass members' PII. This exclusive knowledge includes, but is not limited to, information that Flagstar received through internal and other non-public audits and reviews that concluded that Flagstar's security policies were substandard and deficient, and that Plaintiff's and the Michigan Subclass members' PII and other Flagstar data was vulnerable.

164. Flagstar had exclusive knowledge about the extent of the Data Breach, including during the days, weeks, and months following the Data Breach.

165. Flagstar failed to disclose, and actively concealed, the material information it had regarding Flagstar's deficient security policies and practices, and regarding the security of the sensitive PII and financial information. For example, even though Flagstar has long known, through internal audits and otherwise, that its security policies and practices were substandard and deficient, and that Plaintiff's and the Michigan Subclass members' PII was vulnerable as a result, Flagstar failed to disclose this information to, and actively concealed this information from, Plaintiff, the Michigan Subclass members, and the public. During the days and weeks following the Data Breach, Flagstar failed to disclose, and actively concealed, information that it had regarding the extent and nature of the Data Breach.

166. Flagstar had a duty to disclose the material information that it had because, *inter alia*, it had exclusive knowledge of the information, it actively

concealed the information, and because Flagstar was in a fiduciary position by virtue of the fact that Flagstar collected and maintained Plaintiff's and the Michigan Subclass members' PII and financial information.

167. Flagstar's representations and omissions were material because they were likely to deceive reasonable individuals about the adequacy of Flagstar's data security and its ability to protect the confidentiality of its clients' PII.

168. Had Flagstar disclosed to Plaintiff and the Michigan Subclass that its data systems were not secure and, thus, vulnerable to attack, Flagstar would have been unable to continue in business without adopting reasonable data security measures and complying with the law. Instead, Flagstar received, maintained, and compiled Plaintiff's and the Michigan Subclass members' PII without advising them that Flagstar's data security practices were insufficient to maintain the safety and confidentiality of their PII.

169. For the foregoing reasons, Plaintiff and the Michigan Subclass members acted reasonably in relying on Flagstar's misrepresentations and omissions, the truth of which they could not have discovered.

170. Flagstar's practices were also contrary to legislatively declared and public policies that seek to protect data and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected in the Michigan Identity Theft Protection Act.

171. Flagstar acted intentionally, knowingly, and maliciously in violating the Michigan Consumer Protection Act and the Michigan Identity Theft Protection Act and recklessly disregarded Plaintiff and the Michigan Subclass members' rights. Flagstar's earlier 2021 data breach involving its vendor Accellion, discussed above, put it on notice that its security and privacy protections were inadequate.

172. As a direct and proximate result of Flagstar's unfair, unconscionable, and deceptive practices, Plaintiff and the Michigan Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Flagstar, as they would not have paid Flagstar for goods and services or would have paid less for such goods and services but for Flagstar's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their PII; and an increased, imminent risk of fraud and identity theft.

173. The injuries suffered by Plaintiff and the Michigan Subclass greatly outweigh any potential countervailing benefit to consumers or to competition, and they are not injuries that Plaintiff and the Michigan Subclass should have reasonably avoided.

174. Plaintiff and the Michigan Subclass members seek all monetary and

non-monetary relief allowed by law, including the greater of actual damages or $250, restitution, declaratory and injunctive relief, reasonable attorneys' fees and costs, and any other relief that is just and proper.

175. Therefore, Plaintiff prays for relief as set forth below.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the members of the Class, respectfully requests the Court to enter an Order:

A. certifying the proposed Class under Federal Rule of Civil Procedure 23(a), (b)(2), and (b)(3), as set forth above;

B. declaring that Defendant is financially responsible for notifying the Class members of the pendency of this suit;

C. declaring that Defendant has committed the violations of law alleged herein;

D. providing for any and all injunctive relief the Court deems appropriate;

E. awarding monetary damages, including but not limited to any compensatory, incidental, or consequential damages in an amount that the Court or jury will determine, in accordance with applicable law;

F. providing for any and all equitable monetary relief the Court deems appropriate;

G. awarding punitive or exemplary damages in accordance with proof and

in an amount consistent with applicable precedent;

H. awarding Plaintiff reasonable costs and expenses of suit, including attorneys' fees;

I. awarding pre- and post-judgment interest to the extent the law allows; and

J. providing such further relief as this Court may deem just and proper.

DEMAND FOR TRIAL BY JURY

Plaintiff demands a trial by jury of all issues so triable.

Date: July 26, 2022

Respectfully submitted,

DICELLO LEVITT GUTZLER LLC

By: */s/ Amy E. Keller*
Amy E. Keller
akeller@dicellolevitt.com
Ten North Dearborn Street, Sixth Floor
Chicago, Illinois 60602
Telephone: (312) 214-7900

REESE LLP
Michael R. Reese (*pro hac vice* to be filed)
mreese@reesellp.com
100 West 93rd Street, 16th Floor
New York, New York 10025
Telephone: (212) 643-0500

REESE LLP
George V. Granade (*pro hac vice* to be filed)
ggranade@reesellp.com
8484 Wilshire Boulevard, Suite 515

Los Angeles, California 90211
Telephone: (310) 393-0070

Counsel for Plaintiff and the Proposed Class